UNCLASSIFIED

JADS JT&E

JADS Special Report on Networking and Engineering

By: Charles P. Ashton, MSgt, USAF

August 1999

Distribution A- Approved for public release; distribution is unlimited.

Joint Advanced Distributed Simulation
Joint Test Force
2050A 2nd St. SE
Kirtland Air Force Base, New Mexico 87117-5522

UNCLASSIFIED

Contents

Appendices

List of Figures

List of Tables

1.0 Purpose and Background

1.1 Purpose

This report describes the Joint Advanced Distributed Simulation (JADS) Joint Test Force (JTF) communications network. It outlines the network design requirements, network description, and describes the components. Also, this report addresses JADS JTF costs, concerns and constraints, and lessons learned. It is intended to provide insight into the process JADS JTF undertook in setting up a distributed communications network capable of supporting advanced distributed simulation (ADS) testing.

1.2 Background

The JADS Joint Test and Evaluation (JT&E) was chartered by the Deputy Director, Test, Systems Engineering and Evaluation (Test and Evaluation), Office of the Under Secretary of Defense (Acquisition and Technology) in October 1994 to investigate the utility of ADS technologies for support of developmental test and evaluation (DT&E) and operational test and evaluation (OT&E). The program is Air Force led with Army and Navy participation.

The JADS JTF is directly investigating ADS applications in three slices of the test and evaluation (T&E) spectrum: the Systems Integration Test (SIT) explored ADS support of air-to-air missile testing; the End-to-End (ETE) Test investigated ADS support for command, control, communications, computers, intelligence, surveillance and reconnaissance (C4ISR) testing; and the Electronic Warfare (EW) Test explored ADS support for EW testing. Each test applied the JADS objectives and measures as appropriate to conduct its evaluation.

1.2.1 Systems Integration Test (SIT) Description

The SIT evaluated the utility of using ADS to support cost-effective testing of an integrated missile weapon/launch aircraft system in an operationally realistic scenario. The SIT also evaluated the capability of the JADS Test Control and Analysis Center (TCAC) to control a distributed test of this type and to remotely monitor and analyze test results. The SIT consisted of the Linked Simulators Phase (LSP) and the Live Fly Phase (LFP). The missions simulated a single shooter aircraft launching an air-to-air missile against a single target aircraft. The LSP incorporated a manned F-18 avionics lab (simulator) at China Lake Naval Air Station (NAS) California, as the shooter; a manned F-14 avionics lab (simulator) at Point Mugu NAS California, as the target; and a missile hardware-in-the-loop (HWIL) simulation lab (simulator) at China Lake NAS which generated air intercept missile (AIM)-9 missile flyouts and injected countermeasures (flares). The LFP employed an architecture which incorporated a live F-16 shooter aircraft, a live F-16 target aircraft, and an Advanced Medium Range Air-to-Air Missile (AMRAAM) HWIL simulator hosted in the Eglin Air Force Base (AFB), Florida, Missile Lab.

1.2.2 End-to-End (ETE) Test Description

The ETE Test was designed to evaluate the utility of ADS to support testing of C4ISR systems. The test used the developmental and operational testing issues for the Joint Surveillance Target Attack Radar System (Joint STARS) in an ADS-enhanced environment to conduct its T&E utility evaluation. Also, the ETE Test evaluated the capability of the JADS TCAC to control a distributed test and remotely monitor and analyze test results. The ETE Test consisted of four phases. Phase 1 developed or modified the components that allowed a mix of live and simulated targets at an E-8C operator's console and a light ground station module (LGSM) operator's console. Phase 2 evaluated the utility of ADS to support DT&E and early OT&E of a C4ISR system in a laboratory environment. Phase 3 moved portions of the architecture to the E-8C aircraft, ensured that the components functioned properly, and confirmed that the synthetic environment interacted properly with the aircraft and actual LGSM. Phase 4 evaluated the ability to perform test and evaluation of the E-8C and LGSM in a synthetically enhanced operational environment using typical operators.

1.2.3 Electronic Warfare (EW) Test Description

The EW Test was designed to evaluate the utility of ADS in a distributed EW environment. It consisted of three phases. Phase 1 consisted of open air range and hardware-in-the-loop testing to develop a performance baseline for the two subsequent phases. Phase 2 employed a linked architecture that utilized the Department of Defense's (DoD) high level architecture (HLA) and included a digital system model of the ALQ-131 self-protection jammer, threat simulation facilities, and constructive models that replicated the open air environment. Phase 3 substituted an installed systems test facility (anechoic chamber) with an ALQ-131 pod mounted on an F-16 for the digital systems model. Both Phase 2 and Phase 3 compared system performance data with live fly data from Phase 1 for verification and validation (V&V).

2.0 Network Design Requirements

The network design requirements are broken into four distinct areas: common, SIT, ETE Test and EW Test requirements. The common network requirements were provided by the JADS Steering Committee (leadership). The individual test team requirements were provided by the JADS test teams.

2.1 Common Network Requirements

Although the three JADS JTF test programs were investigating the utility of ADS in distinctly different environments, the following were common requirements of the tests:

- Robust communications architecture with expansion capabilities.
- High reliability with the capability to remotely instrument performance of the communications circuits.
- Exclusive use and management of the bandwidth during periods of test or integration.
- Full control over scheduling of the network. It was determined that additional scheduling requirements increased the risk of conducting a test event. Also, the test teams had a need to respond to unscheduled availability of facilities for integration work.
- Complete management control of the communications network in order to make changes as needed and evaluate the performance of each link in the network.
- With the exception of the SIT, all links had to dedicate at least one 64 kilobits per second (Kbits) time slot for voice communications in support of test control and execution.
- National Security Agency (NSA)-approved communications security (COMSEC) equipment to encrypt the communications circuits.
- Routing equipment support for transmission control protocol (TCP)/internet protocol (IP) for data transmission.
- Routing equipment support for simple network management protocol (SNMP) in order to remotely instrument router performance.
- Routing equipment support for forwarding user datagram protocol (UDP) among all sites.

2.2 Systems Integration Test (SIT) Network Requirements

The SIT network had to support the following:

- Directed broadcasting of distributed interactive simulation (DIS) protocol data units (PDUs).
- Data rates between sites up to 768 Kbits.
- Closed-loop interaction, one-way latency less than 100 milliseconds (ms).
- Open-loop no interaction, one-way latency less than 300 ms.
- 10 megabits per second (Mbps) Ethernet to interconnect the various workstations and router at a site.
- If feasible, use existing network capabilities among sites.

2.3 End-to-End (ETE) Test Network Requirements

The ETE Test network had to support the following:

- Directed and selective broadcasting of DIS PDUs.
- The ability to transmit DIS PDUs from an unclassified network into a classified (secure) network environment.
- Data rates among sites up to 1024 Kbits.
- 10 Mbps Ethernet to interconnect the various workstations and router at a site.

2.4 Electronic Warfare (EW) Test Network Requirements

The EW Test network had to support the following:

- IP multicasting among all sites.
- One-way application-to-application latency less than 150 ms (300 ms round trip).
- Data rates among sites up to 1 Mbps.
- 10/100 Mbps Ethernet to interconnect the various workstations and router at a site.

3.0 Network Descriptions

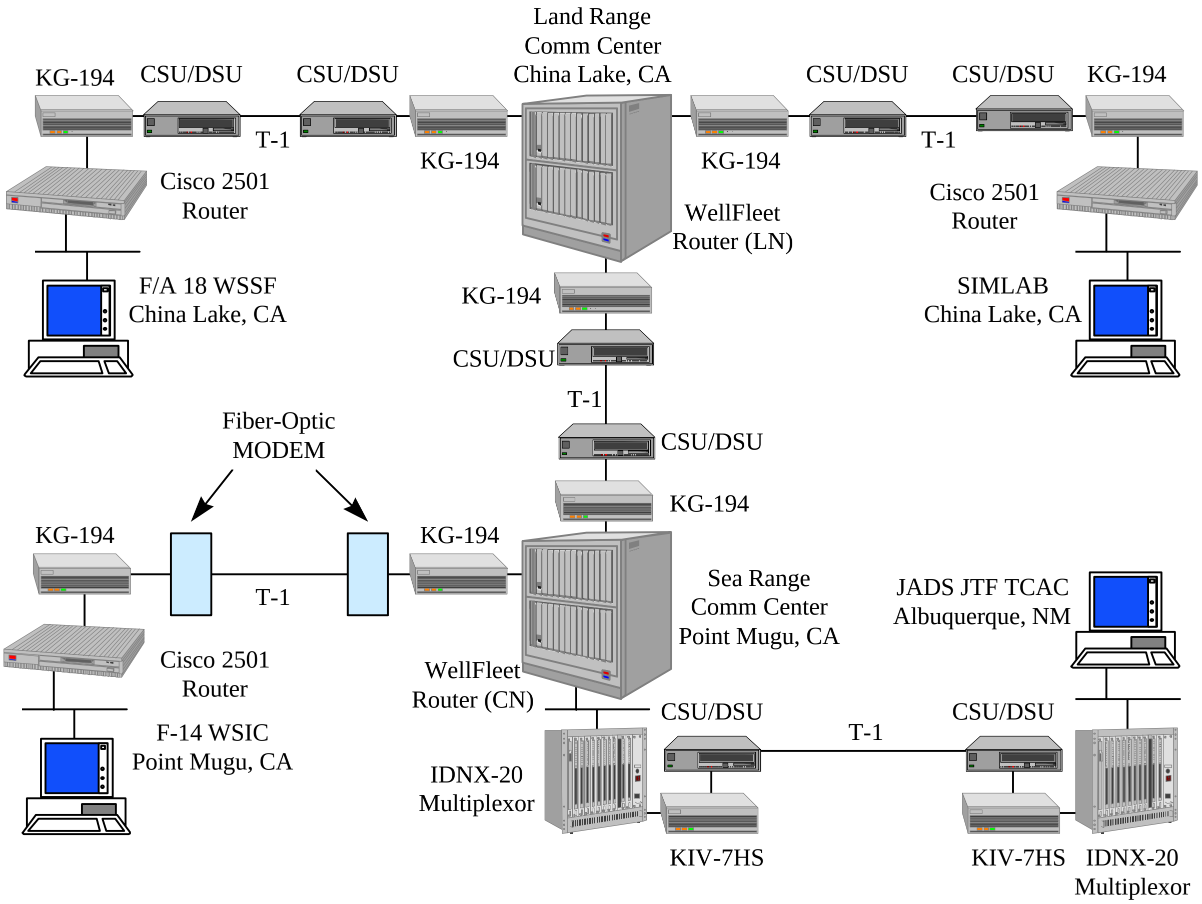
The following sections describe the individual JADS test teams' wide area networks (WAN). The figures represent an overview of the individual WANs and do not depict the network interface units (NIUs), simulators, or local area network (LAN) equipment at each site. Refer to Appendix A for detailed network diagrams.

3.1 Systems Integration Test (SIT)

The SIT was able to utilize existing networking infrastructure for both LSP and LFP. Also, JADS JTF was able to utilize the same networking equipment as the ETE Test and EW Test programs to connect the TCAC in Albuquerque, New Mexico, to the existing networks in Point Mugu and Eglin AFB.

3.1.1 Linked Simulators Phase

Figure 1 details the SIT LSP communications network. The involved facilities at Point Mugu and China Lake were already linked together through the Naval Air Warfare Center Weapons Division (NAWC-WPNS) Near-Real-Time Network (NRNet) at Point Mugu. JADS JTF leased a T-1 line from Albuquerque to Point Mugu and connected into the NRNet at the Sea Range Communications Center. Although the NRNet was pre-existing, it required extensive changes to the routers' configurations (directed broadcasting, routing tables, etc.) to support the SIT networking requirements. These modifications were primarily necessary because of differences in the various models and vendors of the routing equipment. Also, because of latency concerns and NRNet traffic loading, the missile simulator and F/A-18 labs at China Lake had to connect their military standard (MIL STD) 1553B data busses via a separate data circuit in order to get proper interaction between the F/A-18 weapons control system and the missile launch control system.

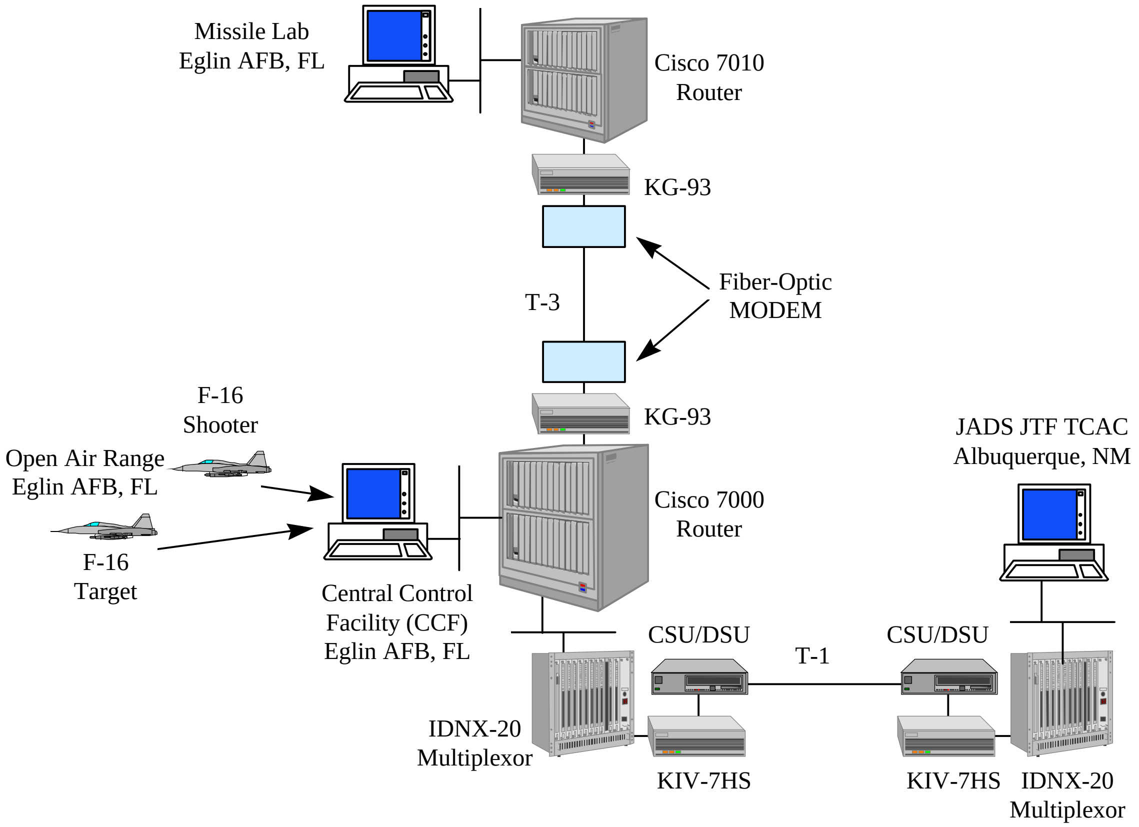


CSU = channel service unit
DSU = data service unit
INDX™ = Integrated Digital Network Exchange
KG = a family of communications security equipment
modem = modulator/demodulator
SIMLAB = Simulation Laboratory
T-1 = digital carrier used to transmit a formatted digital signal at 1.544 megabits per second
WSIC = Weapons System Integration Center
WSSF = Weapon System Support Facility

Figure 1. SIT Linked Simulator Phase Network

3.1.2 Live Fly Phase

Figure 2 details the SIT LFP communications network. The involved facilities at Eglin AFB built a network infrastructure to meet the SIT LFP requirements. JADS JTF leased a T-1 line from Albuquerque to Eglin AFB and connected into Eglin's network at the Central Control Facility (CCF). The network required minor changes once all of the components were installed to optimize network performance and meet the LFP network requirements. The infrastructure and networking equipment at Eglin AFB were left in place as a legacy network for future ADS testing at Eglin AFB.

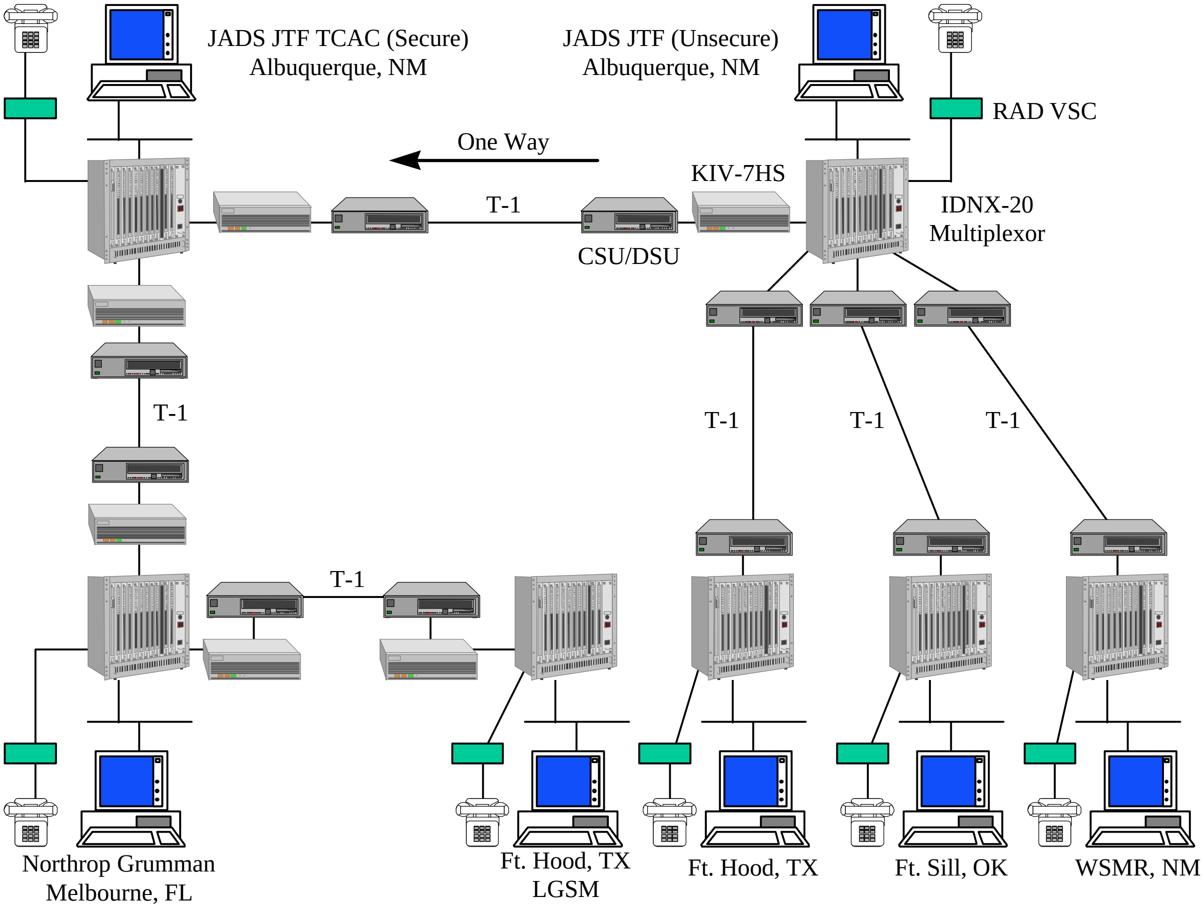


CSU = channel service unit DSU = data service unit INDX™ = Integrated Digital Network Exchange
KG = a family of communications security equipment modem = modulator/demodulator
T- = digital carrier used to transmit a formatted digital signal at 1.544 megabits per second
T-3 = 28 T-1 lines in one; the aggregate data rate is 44.746 megabits per second

Figure 2. SIT Live Fly Phase Network

3.2 End-to-End (ETE) Test

Figure 3 details the ETE Test communications network. The ETE Test presented the challenge of transmitting UDP data from an unclassified site into a classified network. This was accomplished by configuring a one-way only link at the JADS facility. JADS JTF received unclassified (nonsecure) data from White Sands Missile Range (WSMR), New Mexico, and Fort Sill, Oklahoma, and forwarded these data into the TCAC, and prevented any data from the secure network propagating to the nonsecure network.

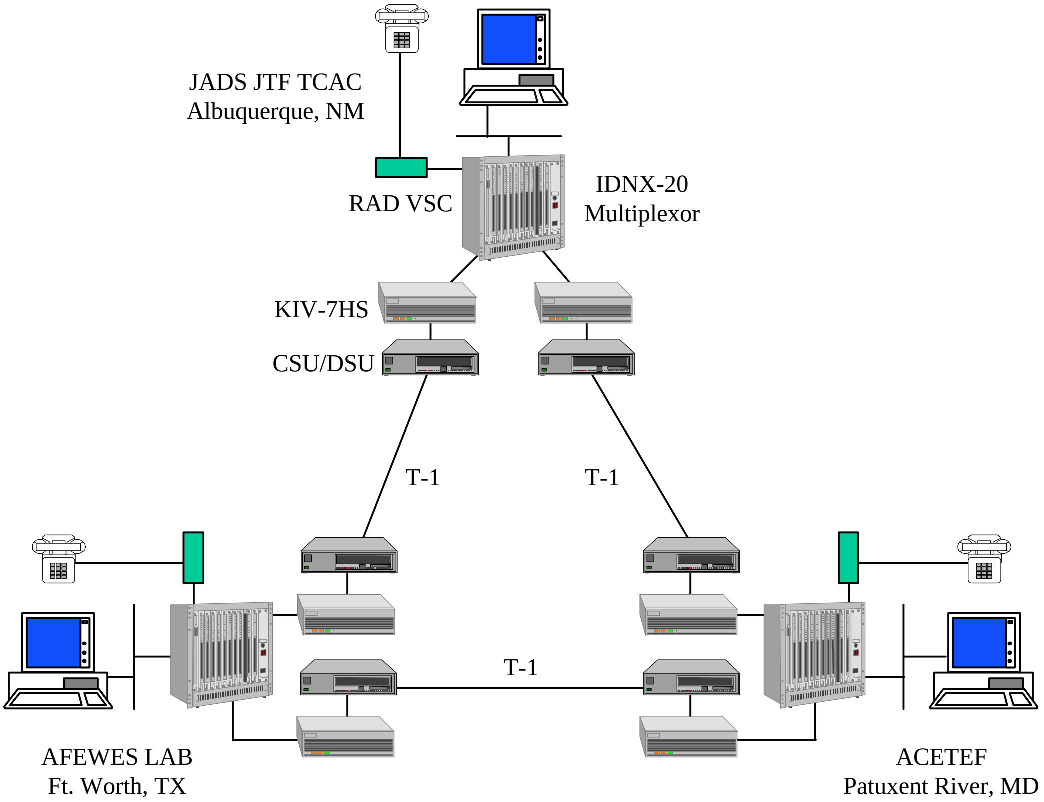


CSU = channel service unit
DSU = data service unit
INDX™ = Integrated Digital Network Exchange
KIV = AlliedSignal embeddable KG-84 communications security
RAD = the company that manufactures the voice signal converter
T-1 = digital carrier used to transmit a formatted digital signal at 1.544 megabits per second
VSC = voice signal converter

Figure 3. ETE Test Network

3.3 Electronic Warfare (EW) Test

Figure 4 details the EW Test communications network. The EW Test presented many challenges in the networking equipment configuration. Although the EW Test was able to utilize the same equipment as the SIT and the ETE Test, the network equipment required extensive configuration changes to optimize the routers' performance while reducing transmission latency to minimal levels.



ACETEF = Air Combat Environment Test and Evaluation Facility
CSU = channel service unit
INDX™ = Integrated Digital Network Exchange
RAD = the company that manufactures the voice signal converter
T-1 = digital carrier used to transmit a formatted digital signal at 1.544 megabits per second
VSC = voice signal converter

AFEWES = Air Force Electronic Warfare Evaluation Simulator
DSU = data service unit
KIV = AlliedSignal embeddable KG-84 communications security

Figure 4. EW Test Network

4.0 Equipment Descriptions

The JADS JTF communications network can be broken down into three distinct segments: the LAN, the WAN, and the Clock Distribution System (CDS). This section will describe the networking equipment installed by the JADS JTF, even though NRNet and Eglin AFB used equipment from other vendors.

4.1 Local Area Network

A variety of LAN technologies were used to support the three JADS JTF test programs. The LANs mainly consisted of hubs and switches. However, Eglin AFB employed a combination of 10 Mbps Ethernet and fiber-optic distributed data interfaces (FDDI). To the extent possible, the LANs contained only equipment directly supporting the JADS tests. This was achieved at all sites except the F-14 Weapons System Integration Center (WSIC) during the SIT LSP. A bridge was used to isolate the JADS equipment from the rest of the WSIC LAN.

4.1.1 Hubs

The hubs were used to interconnect the various computer workstations and the router at a site. JADS JTF utilized a variety of unintelligent 10 Mbps half-duplex Ethernet hubs that were available from multiple vendors.

4.1.2 Switches

The switches were used in the same manner as the hubs to interconnect the computer workstations and the router at a site. The main difference between a switch and a hub is that a switch will selectively route data that its workstations operate at 100 Mbps full-duplex. In order to accommodate this requirement, JADS JTF implemented 10/100Base-T auto-sensing switches that were available from multiple vendors.

4.2 Wide Area Network

Although it was not a requirement, it was desirable to utilize commercial-off-the-shelf (COTS) equipment that was easily obtainable and reasonably affordable. JADS JTF procured all of the WAN equipment through government contracts with significant cost savings compared to the vendors' list prices.

4.2.1 Channel Service Unit/Data Service Unit

The channel service unit (CSU)/data service unit (DSU) interfaces the KIV-7HS encryption device or the Integrated Digital Network Exchange (IDNX™) trunk module to the T-1 communications line by converting the non-return to zero (NRZ) output of the KIV-7HS to a bipolar alternate mark inversion (AMI) signal for transmission over the telecommunications carrier facilities. In addition, the CSU/DSU supports binary eighth zero substitution (B8ZS) encoding and inserts framing bits in the extended super frame (ESF) format. Also, the model (VERILINK AS2000) of CSU/DSU used by the test networks was capable of remote configuration management and monitoring.

4.2.2 KIV-7HS Encryption Device

The KIV-7HS is a NSA-certified link encryption device used to protect the data being transferred between sites. The KIV-7HS protects classified and sensitive digital data transmissions (Type I) at data rates up to 1.544 Mbps. Its performance characteristics are similar to the KG series of cryptographic equipment. The KIV-7HS supports the T-1 data rate with one-way, end-to-end latency of 4.5 microseconds. Also, the primary reason JADS JTF utilized the KIV-7HS was the significant cost savings over the KG series of encryption device. The cost of installing a pair of KIV-7HS encryption devices on a communications circuit was $7,969 versus $20,800 to install a pair of KG-194 encryption devices.

4.2.3 Integrated Digital Network Exchange

IDNX™ is a communications resource manager (CRM), or multiplexer, that supports and integrates a broad range of voice, data, and internetworking services. The entire network can be monitored, managed and controlled from any IDNX™ node in the network. JADS JTF chose the IDNX™-20 series of CRM because of these features and the IDNX™ family of products is extensively used by the Defense Information Systems Agency (DISA) in support of the Defense Information Systems Network (DISN). The ability to configure and manage the systems allowed JADS to quickly troubleshoot problems and reconfigure the network equipment to meet test team requirements. The following subsections only describe the feature modules utilized by the JADS JTF.

4.2.3.1 I422 Trunk Card

The I422 trunk card provides an RS-449/422 compatible interface for the IDNX™ to interface with the KIV-7HS or the CSU/DSU (nonsecure applications). The module also contains a crypto sync relay that allows it to support automatic external resynchronization of encryption equipment. The I422 trunk module does real-time multiplexing, synchronization, inter-nodal signaling, and contains the logic to control allocation of trunk channels. It allocates 16 Kbits of the T-1 bandwidth to an inter-nodal communications channel which is the sole means by which nodes communicate with one another. The channel carries data that allow the network manager to configure, query, and monitor all nodes from anywhere in the network. The inter-nodal channel provides

- Call processing, configuration, network events, and status information to all nodes in the network.
- Code loading when the desired code is not present in the node.
- Database information, events, alarms, and circuit management messages to the network manager.
- Continuous bit error rate test (BERT) in 30 minute intervals on the communications circuit .

4.2.3.2 PX-3 and Access PX Router Modules

The packet exchange (PX) platform is a general purpose router/bridge module integrated into the IDNX™ CRM. The PX platform provides packet-switched services among LANs over a wide area network through the IDNX™ CRM. The module connects the LAN to the WAN via an Ethernet (Institute of Electrical and Electronics Engineers [IEEE] 802.3) or switchable 4/16 Mbps token ring (IEEE 802.5) interface. The PX platform features an onboard processor and up to eight high-speed serial ports. PX platform serial ports can be connected to remote PX modules or to local or remote data cards with external serial ports. The access PX (access packet exchange [APX]) module was used to support the ETE Test and both phases of SIT. The APX utilizes Cisco release 9.1(9) for its operating system. Also, the APX is not year 2000 (Y2K) compliant and does not support IP multicasting. The PX-3 module was implemented for the EW Test. The PX-3 module utilizes Cisco release 11.1 for its operating system. In addition, the PX-3 module supports IP multicasting and is Y2K compliant. JADS JTF used the APX module for the SIT and the ETE Test because the PX-3 module was not available from the vendor at test equipment procurement time.

4.2.3.3 Quad Analog Voice Processor Module

The quad analog voice processor (QAVP) module provides and manages voice calls coming into and leaving the WAN. It serves as the interface between external voice communications equipment and the rest of the network. The QAVP module supports four full-duplex channels, which connect to industry standard 4-wire E&M analog communications equipment. The module converts 3 kilohertz (kHz) bandwidth analog signals to 64 Kbits digital pulse code modulation (PCM) and vice versa. It features echo cancellation, which eliminates echo caused by hybrid transformers that connect two-wire circuits with analog four-wire circuits.

4.2.4 RAD Voice Signal Converter

The RAD voice signal converter (VSC) interfaces between an ordinary 2-wire telephone set and the 4-wire E&M interface enabling direct connection to the analog interface of a time division multiplexer. The VSC recognizes the telephone set pulses for on hook, off hook and dialing, translates the pulses into the proper signaling standard, and sends the resulting signal over the "M" lead. When detecting activity on the "E" lead, the VSC sends the ring signal to the telephone and the ring back tone to the 4-wire E&M interface of the QAVP.

4.3 Clock Distribution System (CDS)

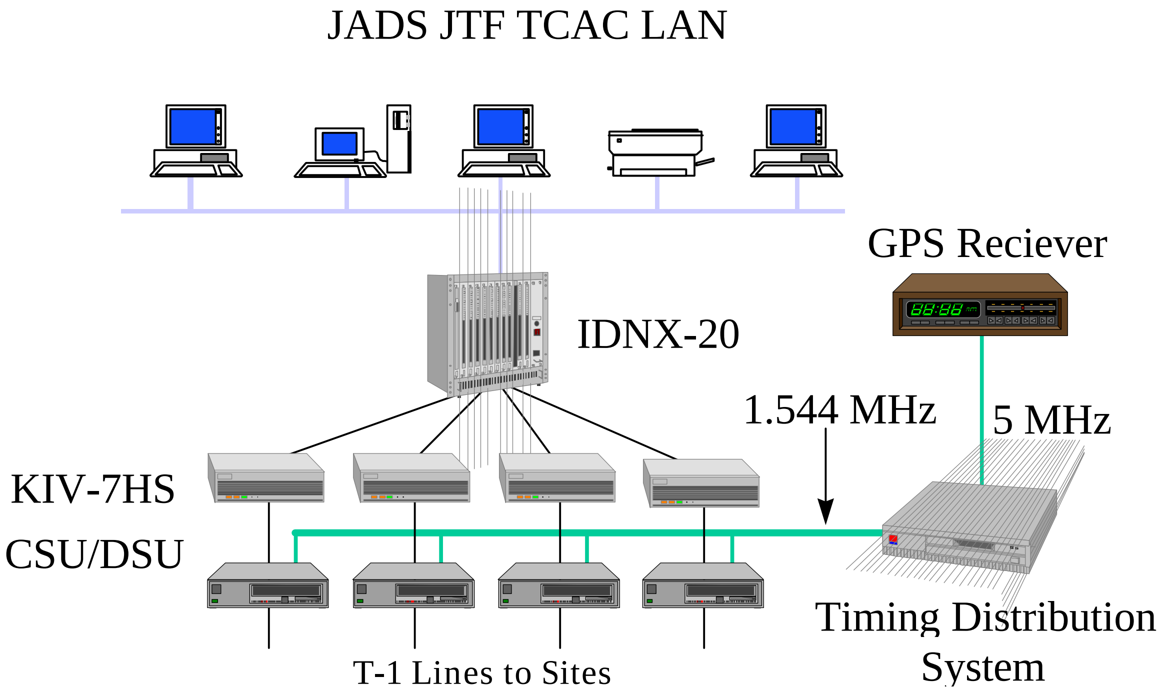
The CDS was used to synchronize all of the WAN equipment to the same timing source. It is vital that the network be slaved to the same timing signal in order to maintain synchronization and prevent bit errors caused by differences in timing in the WAN equipment. The CDS is comprised of three components: the true-time Global Positioning System (GPS) receiver, Fiber Plex Timing Distribution System (TDS), and the CSU/DSUs. Figure 5 depicts how the timing signals were distributed among all the JADS test networks.

4.3.1 True-Time Global Positioning System Receiver

The GPS receiver is a stratum level 1 time source that is provided by the GPS satellite constellation. It has 1 megahertz (MHz), 5 MHz, and 10 MHz signal outputs for use by TDSs. JADS used the 5 MHz signal as the master frequency for input to the TDS.

4.3.2 Fiber Plex Timing Distribution System (TDS)

The Fiber Plex TDS was used to provide and distribute precision local timing to synchronous communications equipment. The TDS accepts the precision timing signals from the GPS receiver and phase locks a local oscillator to the signal. The local oscillator then divides the input frequency down to frequencies usable by the communications equipment. These outputs were wired directly to the external timing inputs of the CSU/DSUs. Then, the CSU/DSUs at the distant sites derived their timing from the incoming data stream from JADS. Figure 5 shows how JADS JTF utilized the CDS.



KIV = AlliedSignal embeddable KG-84 communications security
T-1 = digital carrier used to transmit a formatted digital signal at 1.544 megabits per second

Figure 5. Clock Distribution System

5.0 Network Instrumentation Tools

As part of the requirements definition process, it was deemed essential to evaluate the impact of network performance on test execution. A variety of commercially available tools were evaluated for the capability to perform pretest, real-time, and post-test analysis to evaluate performance of the various test networks and their impact on the quality of collected test data. The network performance areas of primary interest were latency, bandwidth utilization, and data losses. The following sections describe the network instrumentation tools JADS used in evaluating network performance.

5.1 Silicon Graphics, Inc., (SGI) *NetVisualyzerä*

NetVisualyzerä is a network analysis package developed by Silicon Graphics Inc. This product is a suite of protocol analysis tools that can be used during network setup or during testing to ensure that network equipment is configured properly, nodes are talking to one another as intended, and to assist the network manager in identifying, eliminating, or minimizing extraneous network traffic. Remote data stations, located on each LAN segment, collect data and send them to a central display station, where the information is processed by the individual analysis tools and graphically displayed. The additional network load caused by the active data collection over the network was found to be negligible during ETE testing. Traffic flow among specific hosts at each site and among sites is shown near real time, enabling test controllers to quickly realize if link availability among sites is compromised. The ability to monitor current packet rate and load at the LAN level, a valuable asset in evaluating tactical system or simulation activity at an individual site, is offered by another piece of the *NetVisualyzerä* tool set.

5.2 Cabletron *SPECTRUMÒ*

SPECTRUMÒ is a network analysis package developed by Cabletron Systems. It provides a near real-time capability for network traffic monitoring, presenting current packet rate and load information, as well as packet error and discard rate information for network equipment. The package also provides an alarm manager with simple diagnostic capability that is valuable in the detection and troubleshooting of network outages. *SPECTRUMÒ* utilizes the Simple Network Management Protocol (SNMP) to periodically query network devices and displays requested information on screen in table and graphical format. The *SPECTRUMÒ* operator can tailor the destination, frequency, and content of the queries to provide the desired level of insight into a particular network portion or piece of equipment. Like *NetVisualyzerä*, *SPECTRUMÒ* queries for data to create network traffic, although not of appreciable quantity to be noticed in relation to the test traffic. Typically, a five-second polling interval was used to monitor the network equipment, a value chosen so that short duration problem events would most likely not be missed. Multiple databases store *SPECTRUMÒ's* event log and query results for later analysis.

5.3 AG Group, Inc., *EtherPeekä*

EtherPeekä is a network analysis package developed by AG Group Inc. This product is a suite of protocol analysis tools that can be used during network setup or during testing to ensure that network equipment is configured properly, nodes are talking to one another as intended, and to assist the network manager in identifying, eliminating, or minimizing extraneous network traffic. It provides real-time capability for network traffic monitoring, presenting current packet rate and load information, as well as packet error information. Local and remote *EtherPeekä* data stations passively collect all LAN traffic at each site for real-time network analysis. Unlike *NetVisualyzerä* and *SPECTRUM*^{Ò}, *EtherPeekä* does not create any additional network traffic. The protocol analysis part of the tool set was extremely valuable to the EW Test in analyzing latency and data dropouts between nodes.

6.0 Cost

The costs involved in setting up a communications network can be presented a number of different ways. No matter how they are presented, there are two underlying constants that must be accounted for in planning a network. These are communications hardware and circuit costs. A JADS communications node consisted of an IDNX™ CRM, KIV-7HS encryption device, and a CSU/DSU. On average, JADS typically expended approximately $36,000 per site and approximately $90,000 to set up a central communications facility. Communication circuit costs mainly depend upon distance between sites and tariffs imposed by the service provider. Table 1 lists the costs JADS incurred to initially install a circuit (nonrecurring charge or NRC) and the monthly fee thereafter (monthly recurring charge or MRC).

Table 1. Circuit Cost Information

Origination	Destination	NRC	MRC
SIT			
Albuquerque, NM	Point Mugu, CA	$3,763.00	$3,448.00
Albuquerque, NM	Eglin AFB, FL	$2,313.00	$4,604.00
ETE Test			
Albuquerque, NM	WSMR, NM	$0	$700.00
Albuquerque, NM	Fort Sill, OK	$2,500.00	$2,900.00
Albuquerque, NM	Fort Hood, TX	$2,300.00	$3,300.00
Albuquerque, NM	Melbourne, FL	$2,800.00	$4,600.00
Melbourne, FL	Fort Hood, TX	$3,400.00	$3,800.00
EW Test			
Albuquerque, NM	Patuxent River, MD	$1,059.00	$5,527.00
Albuquerque, NM	Fort Worth, TX	$2,457.00	$2,985.00
Ft. Worth, TX	Patuxent River, MD	$1,832.00	$4,873.00

7.0 Concerns and Constraints

7.1 Requirements Definition

Network requirements (i.e., expected data rate, latency budget, communications protocols, control and management of the network) need to be defined early in the process. These requirements must be clearly defined and forwarded to DISA for evaluation of how they can best support the requirements, either through DISA common user networks (i.e., Defense Simulation Internet (DSI), Secret Internet Protocol Router Network (SIPRNET), Defense Research and Engineering Network (DREN), etc.) by granting a waiver exempting use of common user networks in order to build a private network suitable for the requirements. An overview of the different DISA common user networks is contained in Appendix B. It should be noted that if DISA's common user networks are to be used, DISA will allow connection to only one of the networks. These networks cannot be interconnected because of security, interoperability, and tariff constraints. Thus, it requires close coordination with DISA to ensure the network of choice will support all requirements. Network performance data concerning DSI, DSI asynchronous transfer mode (ATM) backbone, and SIPRNET are contained in Appendixes B, C, D, and E.

7.2 Cost

Cost becomes a factor depending upon the networking solution or waiver provided by DISA. The cost of using one of DISA's common user networks may be too high for some customers, depending on which network DISA suggests will meet the requirements. For example, there is a one time NRC of $64,000 to join the DSI with a monthly recurring charge (MRC) of $9,000 per T-1 circuit. Table 2 shows the charges associated with joining SIPRNET. For both networks, the NRC included procurement, installation, and configuration of all necessary equipment. The MRC included operation, configuration management, and maintenance of all equipment and circuits. However, in the case of SIPRNET, the NRC only provided for installation of a central node. Any equipment and/or costs to extend service from that node are the responsibility of the customer.

Table 2. SIPRNET Costs

All Theaters IP Router Service - Monthly Recurring Charges / Fiscal Year 98

Bandwidth:	Ethernet	9.6kB	19.2kB	*56/64kB	128kB	256kB	512kB	1024kB-T-1	E1
Continental United States (CONUS)	$7,748	$1,033	$1,033	$1,033	$1,808	$3,099	$5,165	$6,198	N/A
EUROPE	$10,304	$1,288	$1,288	$1,228	$2,254	$3,864	$6,440	$7,728	$8,372
PACIFIC (HA/AL)	$7,748	$1,033	$1,033	$1,033	$1,808	$3,099	$5,165	$6,198	N/A
PACIFIC RIM	$10,800	$1,350	$1,350	$1,350	$2,363	$4,050	$6,750	$8,100	N/A

*56 kilobytes (kB) available in continental United States (CONUS), 64 kB available for outside the CONUS connectivity.

**NRC for installations: $2,500 for less than 512 Kbits and $5,000 for greater than or equal to 512Kbits.

***Dial-up service equals $50 initiation fee plus $27 per month per comm server access card.

****Dual homing - Second connection of dual homed system will be charged 50% of the MRC that the second connection line speed would ordinarily prompt.

*****The management of customer premise routers (Cisco or Wellfleet routers) have a flat fee of $50 per month for all new customers. All other router management (not Cisco or Wellfleet) will require a specific cost estimate to determine a fee.

7.3 Time

Time is of the essence. Careful planning and consideration must be given to the schedule for implementing the communications network. On average, once the requirements are defined and a networking solution is decided upon, it will take a minimum of 120 days (if a DISA common user network is to be utilized, it could take more than 180 days) to procure and install the necessary communications circuits and networking hardware. Also, it will take a minimum of 90 days to obtain the necessary COMSEC equipment and keying material to encrypt the data. It may take longer if a COMSEC subaccount needs to be established. In addition, time must be allocated in the schedule to install, test, and validate communications network performance. On average, JADS allocated one week per site to accomplish these tasks.

8.0 Lessons Learned

8.1 Planning and Requirements Definition

1. The requirements for an ADS test must be clearly defined early in the test planning phase. Detailed planning and coordination will be required to ensure a common understanding of all requirements, procedures, test objectives, etc., since individual facilities are not generally familiar with conducting coordinated, distributed T&E tests.

2. Network experts must be involved from the beginning. There should be more than one expert, and they must be involved from the beginning of the project to establish the data and instrumentation requirements, verify/validate the networking approach, assist in the development of procedures, and provide overall system expertise.

3. Early definition of network requirements was very advantageous. Having accurate requirements for network connectivity identified early in the program was very advantageous for linking the distributed facilities. JADS network experts estimated the necessary data throughput, encryption, and storage requirements for the ADS network. Their accuracy and resourcefulness allowed them to choose among a few hardware and firmware alternatives, and their early decision making allowed enough time to acquire the right components through government channels and contracting of data circuits through the DISA. This early planning allowed early network integration testing, well ahead of other facility check-outs.

8.2 Network Security

Network security is an essential part of operating an ADS network. The network accreditation process needs to be addressed and started in the planning phase. Security and accreditation procedures are different for every site and branch of service. Hence, it becomes inherently difficult to execute interagency memorandums of agreement (MOA). Security focal points and designated approval authorities need to be identified early in the planning process, and close coordination with these individuals is essential to executing network installation and meeting test schedules. It is wise to factor approximately three months into the implementation schedule to execute the required security MOAs.

8.3 Impact of Network Protocols

8.3.1 User Datagram Protocol (UDP)

UDP is the protocol used by the distributed interactive simulation standard. Since UDP is a broadcast protocol, it is not normally forwarded outside of a LAN. Special consideration must be given to the expected flow of data and interactions among sites in an ADS network in order to properly configure the routing equipment to support the test.

8.3.2 IP Multicasting

IP multicasting is one of the protocols used by the DoD HLA. IP multicasting is a protocol designed to support the broadcasting of information to specific groups of hosts rather than to all hosts on the network. The EW Test used HLA to conduct both Phase 2 and Phase 3. Special consideration had to be given to the different types of data being transmitted during the test in order to determine which data types would be transmitted TCP/IP or IP multicast.

8.4 Network Instrumentation Tools

Network instrumentation tools potentially may have a negative impact on network performance. In particular, a sudden drop in packet rate picked up by Cabletron's *SPECTRUM*^{Ò}, or an altered data traffic pattern on one of the SGI *NetVisualyzer*ä graphs may indicate a network link problem. However, these tools necessarily create additional network traffic with data queries, changing the very nature of the network traffic as they are monitoring it. Taking advantage of the capabilities of simpler tools is one alternative to the trade-off between intrusive monitoring and the need for insight into performance. One nonintrusive solution makes use of the self-diagnostic capabilities of the network equipment. For ETE and EW testing, a line printer in the TCAC facility was set up to print the diagnostic messages directly from the IDNX™ CRM. The sound of the printer would draw immediate attention to a potential equipment outage without intrusive monitoring.

8.5 ADS Network Implementation Guidelines

There were many challenges in designing and implementing a network architecture to support ADS testing. The lessons culminated in the following process that JADS JTF recommends for the design of an ADS-capable network suitable for the T&E community. This section outlines the steps in implementing ADS-based network architecture from a networking point of view.

STEP 1: Define Requirements

Activity 1.1: Identify Sponsor Needs

- Describe critical systems of interest
- Identify resources available to support ADS implementation (e.g., funding, personnel, tools, facilities)
- Identify any known test constraints (e.g., due dates, security requirements)

Activity 1.2: Develop Objectives

- Develop an ADS architecture/network development plan including approximate schedule and major milestones
- Develop a configuration management plan
- Identify security requirements (e.g., classification level and designated approval authority)
- Determine if ADS implementation is appropriate. In general, ADS implementation is necessary if entities interact with each other and if linking is necessary to permit the interactions
- Determine ADS architecture requirements

- Data requirements
  - What data types must be exchanged to permit interaction
  - What data are required to achieve test objectives
  - Rates of data exchanged among entities (in bits per second)
    - Will data be sent out of the simulation interface at the same rate as received by the generating entity or will dead reckoning be used to reduce data rates over the WAN because of WAN bandwidth restrictions
  - Data time stamp accuracy requirement
  - Data classification and security handling requirements
- Latency requirements
  - Acceptable latency and latency variations
  - Closed-loop interaction requirements
- Data quality requirements
  - Acceptable level of ADS-induced errors (e.g., dropout rate, missing PDUs)
  - Data sources and amounts
- Network requirements
  - Protocols to be used
    - Decide whether to use standard protocols (e.g., DIS PDUs) or to keep data in formats generated by entities
  - Will HLA be implemented. Using HLA will affect the choice of protocol and simulation interface design and requires an appropriate runtime infrastructure
  - Will data from nodes be broadcast or transmitted point-to-point. HLA implementation is a factor in this determination
  - Data encryption requirements based on classification of data to be passed over WAN
- Test control and monitoring requirements
  - Test control concept
    - Central control location
    - Test coordinator and location at each distributed node/facility
  - Live entity control technique
    - Is local range control required because of safety considerations or policy
    - Is remote live entity control possible; determine monitoring/communications requirements
  - Display and monitoring requirements
    - Monitoring status of entities
    - Monitoring status/performance of distributed network
  - Voice communications requirements and adequacy of existing telephone systems

STEP 2: ADS Architecture Design

Activity 2.1: Design Architecture

- Determine location of nodes
  - Select simulation facilities based on fidelity, availability, cost, and schedule
  - For live shooter/target configurations, select test ranges based on instrumentation quality and quantity, data processing capability, availability, cost, and schedule
- Conduct surveys of each site (node location)
  - Determine facility communications architecture and requirements
  - Determine physical space requirements for tester-supplied equipment and personnel
- Determine security approach
  - Designate security point of contact
  - Perform security risk assessment and develop concept of operations
- Determine WAN bandwidth requirement
  - For average and maximum aggregate data rate, add rates from each entity broadcast over the WAN
  - Bandwidth requirement equals aggregate data rate plus a 50% - 100% margin for overhead and unanticipated traffic
- Select WAN and LAN
  - DoD-sponsored network or commercial leased lines
    - Consolidate network requirements
      - Acceptable latency limits
      - Aggregate data rates
      - Network management/control
    - Submit requirements to DISA/D36 for determination of whether DISN common user services (e.g., Defense Simulation Internet, SIPRNET) will support the requirements or if a waiver is justified
    - If a waiver is justified, survey commercial line lease rates
      - Dedicated (full-time) leased lines or on-demand leased lines
      - Contract for leased lines
- Select network hardware
  - Type(s) of router(s), CSU/DSU, mulitplexers, etc.
    - If possible, use same type of router for all nodes
    - Router addressing scheme
  - Type(s) of encryptor(s)
- Select test control hardware and software
  - Communications requirements
    - Data communications requirements
    - Voice communications requirements
- Develop formalized plan for architecture development and integration

Activity 2.2: Develop Architecture

- Procure or develop network analysis/monitoring tools
  - Determine required extent of analysis/monitoring
    - Troubleshooting only versus collecting and analyzing data
    - Bandwidth monitoring
      - All versus some links
      - Monitor LANs locally versus remote
    - Hardware requirements (using simple network monitoring protocol)
      - Communications monitoring hardware
  - Obtain permission to monitor or collect data
- Develop procedures for secure/encrypted operations and obtain designated approval authority approval for their use
  - Coordinate security memoranda of agreement with organizations involved
  - Accredit networks, facilities, rooms, etc.
  - Establish communications security account
  - Order keying material
- Implement strict hardware and software configuration control

STEP 3: ADS Architecture Integration and Test

Activity 3.1: Execution Planning

- Develop integration test plan which incrementally checks out configuration during build-up
  - Initially test each WAN link separately
    - First test at CSU/DSU level to make sure communications work at lowest level
    - Use ADS protocols to test routing
    - Use pings to check for connectivity and loading problems
    - Test simulation-to-simulation connections
  - Test simulation-to-simulation connections with all nodes on the network
    - Use network analysis/monitoring tools to troubleshoot the network
    - Use ADS protocols to test routing
- Develop test control procedures
- Develop detailed execution plans.
- For secure networks, develop security test and evaluation plan

Activity 3.2: Integrate and Test ADS Architecture

- Install network hardware and software
- Perform compliance testing
  - Test each facility/node individually to ensure that ADS capability and any required modifications (including software) have been correctly implemented
- Perform integration testing
  - Check out interfaces and facility modifications with linking between pairs of nodes
  - Baseline performance of network with no loading from the simulations/entities
  - Test performance of critical portions of network under loading representative of test conditions to be used

9.0 References

1. Systems Integration Test, Linked Simulators Phase, Final Report, Joint Advanced Distributed Simulation Joint Test and Evaluation, Albuquerque, New Mexico, July 1997

2. Systems Integration Test, Live Fly Phase, Final Report, Joint Advanced Distributed Simulation Joint Test and Evaluation, Albuquerque, New Mexico, March 1998

3. Integrated Digital Network Exchange Technical Documentation, Network Equipment Technologies, Copyright 1995

4. Voice Signaling Converter Installation and Operation Manual, RAD Data Communications Ltd., Copyright 1997

5. Users Manual, Timing Distribution Systems, Buffer Systems, Distribution Amplifiers, Fiber Plex Incorporated, 1997

6. The Utility of Advanced Distributed Simulation for Precision Guided Munitions Testing, Joint Advanced Distributed Simulation Joint Test and Evaluation, Albuquerque, New Mexico, May 1998

7. "Guidance for Complying with ASD(C3I) Policy, 5 May 97, Mandating Use of Defense Information Systems Network (DISN) or FTS Common User Telecommunications Services," HQ DISA message, DTG 121734Z Aug 97

10.0 Acronyms and Abbreviations

ACETEF	Air Combat Environment Test and Evaluation Facility, Patuxent River, Maryland; Navy facility
ADS	advanced distributed simulation
AFB	Air Force base
AFEWES	Air Force Electronic Warfare Evaluation Simulator, Fort Worth, Texas; Air Force managed with Lockheed Martin Corporation
AG	AG Group, Inc.
AIM	air intercept missile
ALQ-131	a mature self-protection jammer system; an electronic countermeasures system with reprogrammable processor developed by Georgia Technical Research Institute
AMI	alternate mark inversion
AMRAAM	advanced medium range air-to-air missile
APX	access packet exchange
ATM	asynchronous transfer mode
B8ZS	binary 8th zero substitution
BERT	bit error rate test
C4ISR	command, control, communications, computers, intelligence, surveillance and reconnaissance
CCF	Central Control Facility
CDS	Clock Distribution System
COMSEC	communications security
CONUS	continental United States
COTS	commercial off-the-shelf
CRM	communications resource manager
CSU	channel service unit
DIS	distributed interactive simulation
DISA	Defense Information Systems Agency
DISN	Defense Information Systems Network
DoD	Department of Defense
DREN	Defense Research and Engineering Network
DSI	Defense Simulation Internet
DSU	data service unit
DT&E	developmental test and evaluation
E&M	analog voice signaling standard
ESF	extended super frame
ETE	End-to-End Test
EW	Electronic Warfare Test
FDDI	fiber distributed data interface
GPS	global positioning system
HLA	high level architecture
HWIL	hardware-in-the-loop (system integration references)

IDNX™	Integrated Digital Network Exchange
IEEE	Institute of Electrical and Electronics Engineers
IP	internet protocol
JADS	Joint Advanced Distributed Simulation, Albuquerque. New Mexico
Joint STARS	Joint Surveillance Target Attack Radar System
JT&E	joint test and evaluation
JTF	joint test force
kB	kilobytes
Kbits	kilobits
KG	a family of communications security equipment
kHz	kilohertz
KIV-7	AlliedSignal embeddable KG-84 communications security module
LAN	local area network
LFP	live fly phase
LGSM	light ground station module
LSP	linked simulators phase
Mbps	megabits per second
MHz	megahertz
MIL-STD	military standard
MOA	memorandum of agreement
modem	modulator/demodulator
MRC	monthly recurring charges
ms	millisecond
NAS	naval air station
NAWC-WPNS	Naval Air Warfare Center Weapons Division
NetVisualizer™	software that displays real-time bandwidth use in a rolling bar graph format for quick visual reference
NIU	network interface unit
NRC	nonrecurring charges
NRNet	Near-Real-Time Network
NRZ	non-return to zero
NSA	National Security Agency
OT&E	operational test and evaluation
PCM	pulse code modulation
PDU	protocol data unit
PX	packet exchange
QAVP	quad-analog voice processor
RAD	the company that manufactures the voice signal converter
SGI	Silicon Graphics, Inc.
SIMLAB	Simulation Laboratory at the Naval Air Warfare Center, China Lake, California
SIPERNET	Secret Internet Protocol Router Network
SIT	System Integration Test
SNMP	Simple Network Management Protocol
SPECTRUM®	an instrumentation suite used to measure bandwidth utilization

T&E	test and evaluation
T-1	digital carrier used to transmit a formatted digital signal at 1.544 megabits per second
T-3	28 T-1 lines in one; the aggregate data rate is 44.746 megabits per second
TCAC	Test Control and Analysis Center at JADS, Albuquerque, New Mexico
TCP	transmission control protocol
TDS	Timing Distribution System
UDP	user datagram protocol
V&V	verification and validation
VSC	voice signal converter
WAN	wide area network
WSIC	Weapons System Integration Center at Naval Air Warfare Center, Point Mugu, California
WSMR	White Sands Missile Range, New Mexico
WSSF	Weapon System Support Facility, China Lake, California
Y2K	year 2000